

Порождающие тройки инволюций группы $GL_n(\mathbb{Z})$.

Основным результатом работы является

Теорема 1. *Группа обратимых $(n \times n)$ матриц $GL_n(\mathbb{Z})$ над кольцом целых чисел \mathbb{Z} , порождается тремя инволюциями, две из которых перестановочны тогда и только тогда, когда $n > 4$.*

1. Обозначения и вспомогательные результаты.

Через $t_{ij}(k)$, $k \in \mathbb{Z}$, $i \neq j$, будем обозначать трансвекции, т.е. матрицы $E_n + ke_{ij}$, где E_n – единичная $(n \times n)$ -матрица, а e_{ij} – матричные единицы.

Обозначим: $\alpha^\beta = \beta\alpha\beta^{-1}$, $[\alpha, \beta] = \alpha^{-1}\beta^{-1}\alpha\beta$. Хорошо известна:

Лемма 1. *Группа $SL_n(\mathbb{Z})$ порождается трансвекциями $t_{ij}(1)$, $i \neq j$, $i, j = 1, 2, \dots, n$.*

Положим:

$$\mu = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & 0 & 1 & 0 \end{pmatrix}.$$

Матрица μ имеет порядок n и действует сопряжениями регулярно на следующем множестве трансвекций:

$$M = \{t_{1n}(1), t_{i+1i}(1), i = 1, 2, \dots, n-1\}.$$

Коммутируя между собой трансвекции из множества M , можно получить все трансвекции $t_{ij}(1)$. Следовательно, множество M порождает группу $SL_n(\mathbb{Z})$. Более того, справедлива:

Лемма 2. *Группа $SL_n(\mathbb{Z})$ порождается одной из трансвекций*

$$t_{1n}(1), t_{i+1i}(1), t_{n-1n}(1), t_{ii+1}(1), i = 1, 2, \dots, n-1,$$

и мономиальной матрицей $\eta\mu$ для любой $(1, -1)$ -диагональной матрицы η с условием, что $\eta\mu \in SL_n(\mathbb{Z})$ [2].

Под $(1, -1)$ -диагональной матрицей понимается диагональная матрица с элементами ± 1 по диагонали.

Лемма 3. *Группа $GL_n(\mathbb{Z})$ порождается трансвекциями $t_{ij}(1)$, $i \neq j$, $i, j = 1, 2, \dots, n$, и любой другой матрицей с определителем -1 [1].*

Предложение 1. Группа $GL_3(\mathbb{Z})$ порождается тремя инволюциями:

$$\alpha = \begin{pmatrix} -1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Доказательство. Так как определитель матрицы α равен -1 (как, впрочем, и двух других) и

$$\alpha\beta = \mu \text{ при } n=3;$$

$$\alpha^\beta = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad \alpha^\mu = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \quad (\alpha\alpha^\mu)^2 = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix},$$

$$\alpha^\gamma = \begin{pmatrix} 1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad (\alpha^\gamma)^\alpha = \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \varepsilon, \quad (\varepsilon\gamma)\alpha^\beta = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 1 & 0 & 1 \end{pmatrix} = \zeta,$$

$$(\zeta^2)^\beta = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad ((\alpha\alpha^\mu)^2)((\zeta^2)^\beta) = t_{31}(1).$$

Следовательно, по лемме 3 инволюции α, β, γ порождают группу $GL_3(\mathbb{Z})$, ч.т.д.

Предложение 2. Группа $GL_4(\mathbb{Z})$ порождается тремя инволюциями:

$$\alpha = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad \beta = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Доказательство. Так как определитель матрицы γ равен -1 (как, впрочем, и β) и

$$\alpha\beta = \mu \text{ при } n=4;$$

$$\gamma^\beta = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \gamma^\mu = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad (\gamma\gamma^\mu)^2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$\begin{aligned}
\gamma^\alpha &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & -1 \end{pmatrix}, & (\gamma^\beta)^{\beta\gamma} &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \eta, & (((\gamma^\beta)^\alpha))^\gamma &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ -2 & -1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \xi, \\
\eta(\xi((\gamma^\mu)^2)) &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \zeta, & (\zeta\gamma)\gamma^\beta\gamma &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} = \varepsilon, & \varepsilon\alpha\gamma^\beta &= \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & -1 & -1 & 0 \\ 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix} = \theta, \\
((\gamma^\mu)^2)((\theta^2\gamma^\alpha)^2)^\alpha &= t_{31}(1), \\
((t_{31}(1))\gamma^\beta) &= t_{21}(1).
\end{aligned}$$

Следовательно, по лемме 3 инволюции α, β, γ порождают группу $GL_4(\mathbb{Z})$, ч.т.д.

Однако при $n=3$ и $n=4$ порождающие инволюции не перестановочны.

Перейдем к доказательству теоремы.

2. Порождающие тройки инволюций при $n > 4$.

Подберем инволюции α, β, γ так, чтобы $\alpha\beta=\beta\alpha$, а определитель γ был равен -1, иначе мы попадаем в специальную линейную группу.

При $n=2(2k+1)$, $n=4k+1$ (5, 6, 9, 10, ...)

$$\alpha = \begin{pmatrix} -1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 1 & 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & -1 & \dots & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 & 1 \\ 0 & 0 & 0 & \dots & 0 & 0 & -1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 0 & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 & 0 \\ 0 & 0 & 0 & \dots & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & \dots & 0 & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 & 0 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 1 & 0 \\ 0 & 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & -1 \end{pmatrix}.$$

При $n=2(2k+1)+1$, $n=4k$ (7, 8, 11, 12, ...)

$$\alpha = \begin{pmatrix} -1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 1 & 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & -1 & \dots & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 & 1 \\ 0 & 0 & 0 & \dots & 0 & 0 & -1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 0 & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 & 0 \\ 0 & 0 & 0 & \dots & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & \dots & 0 & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 & 0 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 1 & 0 \\ 0 & 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & 1 \end{pmatrix}.$$

3. Доказательство теоремы 1 при $n=2(2k+1)$, $n=4k+1$.

Инволюции α и β перестановочны, кроме того, определитель γ равен -1. Следовательно, надо получить трансвекцию вида:

$$t_{1n}(1), t_{i+1i}(1), t_{n-1n}(1), t_{ii+1}(1), i = 1, 2, \dots, n-1.$$

$$\beta\gamma = \eta = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 0 & -1 \\ 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 & 0 \end{pmatrix}$$

1. $\alpha^\eta = \text{diag}(-1, -1, E_{n-2})t_{32}(1)t_{n1}(-1)$
2. $[\alpha, \alpha^\eta] = t_{31}(-1)t_{(n-1)1}(-1)$
3. $\alpha^{\eta_2} = \text{diag}(1, -1, -1, E_{n-3})t_{12}(1)t_{43}(1)$
4. $\theta = [([[\alpha, \alpha^\eta]\alpha^{\eta_2})^\eta], [\alpha, \alpha^\eta]] = t_{(n-2)1}(-1)t_{(n-1)1}(1)t_{n1}(1)$
5. $[\alpha, \theta] = t_{(n-2)1}(-2)t_{(n-1)1}(3)$
6. $[\alpha, \theta]^\beta = t_{2n}(3)t_{3n}(-2)$
7. $[\alpha, ([\alpha, \alpha^\eta]\theta)^{\eta_2}]^{\eta_3} = t_{2n}(1)t_{3n}(-2)$
8. $([\alpha, ([\alpha, \alpha^\eta]\theta)^{\eta_2}]^{\eta_3})([\alpha, \theta]^\beta)^{-1} = t_{2n}(-2)$
9. $(t_{2n}(-2))^\beta = t_{(n-1)1}(-2)$
10. $\delta = (t_{(n-1)1}(-2))^{-1}[\alpha, \alpha^\eta] = t_{31}(-1)t_{(n-1)1}(1)$

$$11. \zeta = ([\alpha, \alpha^\eta]\theta)[\alpha, [\alpha, \alpha^{\eta^\eta}]\delta^{-1} = t_{(n-1)2}(1)t_{n2}(-1)$$

$$12. \xi = ((\zeta)^{\eta^{-1}})^\beta [\alpha, \theta]^\beta = t_{2n}(1)t_{3n}(-1)$$

$$13. (\xi(t_{2n}(-2))^{-1})^{-1}[\alpha, \theta]^\beta = t_{3n}(-1)$$

$$14. (t_{3n}(-1))^{-1} = t_{3n}(1)$$

$$15. \xi t_{3n}(-1) = t_{2n}(1)$$

$$16. (t_{2n}(1))^\beta = t_{(n-1)1}(1)$$

$$17. (t_{(n-1)1}(1))^\eta = t_{n2}(1)$$

$$18. [t_{3n}(1), t_{n2}(1)] = t_{32}(1).$$

Следовательно, выполняются условия леммы 3, теорема доказана для $n=2(2k+1)$, $n=4k+1$.

4. Доказательство теоремы 1 при $n=2(2k+1)+1$, $n=4k$.

Проводится аналогично предыдущему случаю для соответствующих инволюций α , β , γ .

Необходимо проверить, выполняются ли условия леммы 3.

Определитель γ равен -1. Достаточно получить трансекцию вида:

$$t_{1n}(1), t_{i+1i}(1), t_{n-1n}(1), t_{ii+1}(1), i = 1, 2, \dots, n-1.$$

$$\beta\gamma = \mu = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 & 0 \end{pmatrix}$$

$$1. \alpha^\mu = \text{diag}(-1, -1, E_{n-2})t_{32}(1)t_{n1}(1)$$

$$2. [\alpha, \alpha^\mu] = t_{31}(-1)t_{(n-1)1}(1)$$

$$3. [\alpha, \alpha^\mu]^\mu = t_{42}(-1)t_{n2}(1)$$

$$4. [\alpha, [\alpha, \alpha^\mu]^\mu] = t_{41}(1)t_{(n-1)1}(-1)t_{(n-2)1}(-1)t_{n1}(1)t_{n2}(2)$$

$$5. [\alpha, [\alpha, \alpha^\mu]^\mu]^\mu = t_{(n-2)1}(-1)t_{(n-1)1}(2)t_{3n}(1)t_{(n-2)n}(-1)t_{(n-1)n}(1)$$

$$6. \delta = [[\alpha, \alpha^\mu], [\alpha, [\alpha, \alpha^\mu]^\mu]^\mu] = t_{(n-2)1}(-1)t_{(n-1)1}(1)$$

$$7. \theta = [[\alpha, \alpha^\mu]^\mu, [\alpha, [\alpha, \alpha^\mu]^\mu]^\mu] = t_{32}(-1)t_{(n-2)2}(1)t_{(n-1)2}(-1)$$

$$8. [\alpha, \theta] = t_{31}(-1)t_{(n-2)1}(1)t_{(n-1)1}(-1)$$

$$9. \xi = [\alpha, \theta][\alpha, \alpha^\mu] = t_{(n-2)1}(1)t_{(n-1)1}(-2)$$

$$10. \delta\xi = t_{(n-1)1}(-1)$$

$$11. (t_{(n-1)1}(-1))^{-1} = t_{(n-1)1}(1)$$

$$12. (t_{(n-1)1}(1))^\mu = t_{n2}(1)$$

$$13. ((t_{n2}(1))\alpha^\gamma)^2 = t_{12}(1).$$

Условия леммы 3 выполняются, так как искомая трансвекция получена, следовательно, теорема доказана.

5. Порождающие мультиплеты инволюций.

Для группы G через $n(G)$ обозначим минимальное число порождающих инволюций, произведение которых равно 1. Ясно, что если G' — гомоморфный образ G , то $n(G') \leq n(G)$.

Лемма 4. Если $n(G) = 4$, то в G найдется нетривиальная циклическая нормальная подгруппа.

Доказательство леммы 4. Пусть $G = \langle \alpha, \beta, \gamma \rangle$, $n(G) = 4$, и $\alpha, \beta, \gamma, \delta$ — порождающие инволюции, произведение которых равно 1, причем $\delta = \alpha\beta\gamma$. Покажем, что $I \neq H = \langle \alpha\beta \rangle$ — нетривиальная циклическая нормальная подгруппа G , порожденная инволюцией $\alpha\beta$. Действительно,

1. $H^\alpha = \langle \alpha\alpha\beta\alpha \rangle = \langle \beta\alpha \rangle = H$;
2. $H^\beta = \langle \beta\alpha\beta\beta \rangle = \langle \beta\alpha \rangle = H$;
3. δ — инволюция, к тому же $\delta = \alpha\beta\gamma$, следовательно, $(\alpha\beta\gamma)(\alpha\beta\gamma) = I$. Но, с другой стороны, в силу ассоциативности умножения матриц $(\alpha\beta)(\gamma\alpha\beta\gamma) = 1$, а значит $(\alpha\beta)^\gamma = \beta\alpha$. Итак, $H^\gamma = H$.

В итоге H — нормальная (циклическая) подгруппа группы G , лемма доказана.

Из леммы 4 вытекает:

Лемма 5. Если G — конечная простая не абелева группа, то $n(G) \geq 5$.

Теорема 2. Пусть $G = GL_n(Z)$. Тогда:

- 1) $n(G) = 6$ при $n=2,3,4$;
- 2) $n(G) = 5$ при $n>4$.

6. Доказательство теоремы 2.

1) Известно, что

$$1.1. n(GL_2(Z)) = 6 [1];$$

$$1.2. n(SL_3(2)) = 6 [2], n(SL_4(2)) = 6 [3];$$

1.3. Существует гомоморфизм $GL_n(Z) \rightarrow GL_n(2)$;

1.4. $GL_3(Z)$, $GL_4(Z)$ порождаются тремя инволюциями по предложениям 1 и 2 соответственно.

Из 1.4. следует, что $n(GL_3(Z)) \leq 6$, $n(GL_4(Z)) \leq 6$, а из 1.3. – при $n=3,4$ $GL_3(Z) \rightarrow GL_3(2)$, $GL_4(Z) \rightarrow GL_4(2)$. Но, с другой стороны, $GL_n(2) = SL_n(2)$, а значит $GL_3(Z) \rightarrow SL_3(2)$, $GL_4(Z) \rightarrow SL_4(2)$. Так как, если G' – гомоморфный образ G , то $n(G') \leq n(G)$, то $6 \leq n(GL_3(Z))$, $6 \leq n(GL_4(Z))$. Поучаем неравенства $6 \leq n(GL_3(Z)) \leq 6$, $6 \leq n(GL_4(Z)) \leq 6$. Ясно, что это возможно лишь при $n(GL_3(Z)) = 6$, $n(GL_4(Z)) = 6$.

2) По теореме 1 $GL_n(Z)$ при $n > 4$ порождается тремя инволюциями, две из которых перестановочны, следовательно, порождается и пятью инволюциями $\alpha, \beta, \gamma, \gamma, \beta\alpha$, а значит $n(GL_n(Z)) \leq 5$. Предположим, что $n(GL_n(Z)) = 4$, и $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ – порождающие инволюции, произведение которых равно 1. Тогда из равенств $GL_n(2) = SL_n(2) = PSL_n(2)$ и существования гомоморфизма $GL_n(Z) \rightarrow GL_n(2)$, следует, что при $n > 4$ $n(PSL_n(2)) \leq 4$. Но так как $PSL_n(2)$ – простая группа, то в силу леммы 5 $n(PSL_n(2)) \geq 5$. Получили противоречие. В итоге, $n(GL_n(Z)) = 5$, теорема доказана.

Литература.

- [1] Я. Н. Нужин, И. А. Тимофеев, Порождающие тройки инволюций линейных групп размерности 2 над кольцом целых чисел, Владикавказский математический журнал, 2009, Том 11, выпуск 4.
- [2] Я. Н. Нужин, О порождаемости группы $PSL_n(Z)$ тремя инволюциями, две из которых перестановочны, Владикавказский математический журнал, 2008, Том 10, Выпуск 1.
- [3] В. А. Шмидт